EARTO Position Paper on Research Security
- Inputs to the EC Call for Evidence for EC proposal for a Council Recommendation -

3 January 2024

EARTO sees the new European Commission Proposal for a European Economic Security Strategy as an opportunity to improve research security and reduce risks related to the international nature of scientific research and technological development, and especially those related to undesirable transfer of knowledge, foreign interference, and ethical or integrity violations. Looking at the importance of such topics, EARTO is concerned by the short response time given to answer the EC current open call for evidence for EC proposal for a Council Recommendation on research security. In any case, EARTO members are happy to bring forward their views on the guiding principles and key policy actions to support strengthening research security in Europe.

As a reminder, Research and Technology Organisations (RTOs) are non-profit organisations whose core mission is to produce, combine and bridge various types of knowledge, skills and infrastructures to deliver a range of research and development activities in collaboration with public and industrial partners of all sizes. These activities aim to result in technological and social innovations and system solutions that contribute to and mutually reinforce their economic, societal and policy impacts[1]. Accordingly, RTOs' research inherently has an IPR potential and, as such, needs to be secured.

RTOs & Research Security

RTOs have responsible business practices including due diligence. They comply with all EU and national laws and regulations such as export control requirements and international trade controls. RTOs have very good and close cooperation with their national authorities on security issues. In addition, RTOs have a Code of Conduct and expect clients to abide by their codes of conduct. Still, more efforts need to be made, such as raising awareness, providing more training, more guidance for the grey areas, and regarding the ever-increasing threats and risks (e.g. in recruitment, partnerships, investments, procurement). There is also a need to reach a common understanding in the whole RD&I community: the last ERA workshop held on 15 December focused mainly on academics, and there is work to do to look at the other RD&I actors in the EU ecosystem. In addition, despite facing similar threats and sharing common needs and goals, each Member State defines on its own which themes and subjects are considered as sensitive at national level and consequently decides which scientific, research, and technical heritage should be protected. Member States have their own regulations developed with their own methodologies and tools assessing the security risks. Furthermore, to abide by their national regulations and frameworks, RTOs have also their own internal verification processes, considering national recommendations and commonly shared good practices (for example: due diligence on companies, on shareholders' committees and boards of directors, or financing). Finally, RTOs also regularly raise awareness among their staff, at all hierarchic levels, especially about the risks of capturing sensitive knowledge and technologies (i.e. internal training and awareness campaigns). RTOs also maintain an open dialogue with their government, sharing the "signals" they identify and receiving directives, recommendations, and alerts.

Guiding principles on Research Security

EARTO members would like to make the following guiding principles for research security:

1. **Strike the right balance between international collaboration and knowledge protection**

The scientific actors generally consider international collaboration as an absolute priority but remains insufficiently aware of the risks of unbalanced collaborations or of their knowledge being used to increase military power or undermine fundamental freedoms. If the freedom of research and the universal sharing of knowledge remains fundamental, it is essential to evaluate collaborations and exchanges from the point of view of protecting knowledge and technology to ensure the necessary balance between the various parties, all the while preserving this freedom. The right balance between international collaboration and knowledge protection must be found. When creating new legislation or framework on

[1] OECD Definition, see OECD report by P. Larrué &Al, 2022.

research security, the implications for governmental institutions as well as for private organisations need to be taken into account (e.g. on how to handle classified information).

2. **Set a level-playing-field for research security across Europe: Exchange of best practices to promote the creation of a common European framework**

Member States should aim to define a common European framework with security guidelines based on each country's regulations on the protection of their scientific and technical assets. Such a common framework could look at common certification, how data are treated, exchanges on best security practices developed, comparison of national methodologies (e.g. on how to define dual-use technologies or on how to conduct prior analysis). Member States should also look further at how to share the outcomes from their security investigations in a way that ensures anonymity and confidentiality but allows the community to go a step further in terms of security.

In this context, EARTO would like to point out that multilateral dialogues with non-EU countries are for now too sensitive when discussing Research Security while we are at a stage of defining our own framework for research security. In this context, the future activities undertaken under ERA Actions should be better connected with the current European economic security strategy and critical technology prioritisation (e.g. within CRMA, STEP, etc.).

3. **Fundamental research should not be less overwatched**

While fundamental research might appear less risky, it must not be subject to less vigilance. Resolving global issues through increased international cooperation in fundamental research is of importance. However, Europe should not lose sight of the potential security risks attached to fundamental research (i.e. loss of ownership of results, malicious use, dual use). As fundamental research is also subject to regular attempts of interferences and leakages, special attention must be paid to it in the same way as to applied research and technologies. Moreover, EU calls should refer to the importance of compliance with research security when it comes to open research infrastructure and research exchanges.

Academic freedom (i.e. the ability to choose your own topics of research) does not apply to many researchers working outside academia and still performing fundamental research. Accordingly, instead of focusing on academic freedom, "ethics in research" should be the focus and safeguarded to avoid undue pressures and foreign interference and ensure research security also in fundamental research. For this, good scientific practices should be followed (i.e. The European Code of Conduct for Research Integrity).

Key actions: Risk analysis as a cornerstone of research security approach at all levels

Risk analysis aims to ensure that the players with whom we collaborate properly interpret our values in terms of freedom of research and the universal sharing of knowledge and do not use them to destabilise or serve conflicting interests.

Accordingly, EARTO members would like to bring forward the following principles on risk analysis, based on self-governance:

1. **The analysis should be conducted on a case-by-case basis:** Each research topic, each proposed collaboration is studied to measure the benefits for the organisation and identify the potential risks. If the level of risk exceeds the expected benefit, a decision is taken not to commit.
2. **The analysis must be graduated according to the issues at stake and depending on the phase of the research**. A distinction must be made between research topics shared upstream, open exchanges at the start of a project and at the end of the research, and research in progress, which needs to be protected for the time it takes to interpret it and produce the associated publications or subsequent patents. A secure by design approach is needed, creating mitigation measures in case of human error.
3. **Decisions should be taken collectively** by the safety department of organisations, in a systematic close dialogue with laboratories, researchers, international relations managers, organisation's senior management, and possibly shared with EU partners in the case of EU consortia. This approach makes it possible to consider the need for laboratories to be open, but also to integrate the risks into the final decision taken. Where appropriate, a decision is made based on the hierarchical level required.
4. **Researchers' awareness should be raised.** Researchers should be asked as early as possible about the possibility of their research being misused and need support in this questioning, providing them concrete examples, depending on their scientific field, of how other players can use their knowledge for malicious purposes. Moreover, decision making of the team leaders and researchers at the front-line must be supported (i.e. visits, recruitment, partnerships, projects). Awareness raising towards researchers and staff is to be done at all levels: within RD&I institutions, managing institutions at national and EU level.
5. **Concerns over financial transparency.** Whereas there is already a check on Ownership and Control for applicants in specific programmes (i.e. EU Defence Fund) or for some sensitive topics under Article 22.5 in Horizon Europe to avoid potential foreign interferences, RTOs, and

individuals are no longer allowed to access the information on the Ultimate Beneficial Owner (UBO) in all verification tools and international financial databases. This decision from the EU Court of Justice is detrimental to EU RD&I actors who are now under the impossibility to be fully informed of their partners and clients.

6. **Balance needed between security and its associated costs:** the right balance between security and not placing empty administrative burden/extra costs on researchers and their employers must be searched. Any new requirements in future EU projects will come at a cost for research performing organisations that will increase their overheads (already not fully financed). So, the EC should ensure that new measures are proportional and implementable. Here it should be avoided that some actors who could not afford some measures, would then be left off (or parts of) the programme.

Suggestions for EU-level Initiatives on Research Security

EARTO welcomes the EC attempt to lead to stimulate open discussions on security at EU level. Various initiatives could be taken at EU level in this field such as:

1. **Raise awareness of the EU RDI community**: starting from the one engaged in the EU funding programmes with training, examples, and guiding principles for the grey areas (e.g. partnerships, procurement, foreign investments, HR). We need a new culture of in the whole research and innovation community and a common understanding of the risks of foreign interference, technology security, and technology leakage.
2. **Comprehensively review practices in Horizon Europe projects**. Currently, conflictual requirements by public funders (sometimes even within different parts of Horizon Europe), e.g. require openness of research infrastructures for projects with clear dual use and/or high-risk countries; clear guidance and tools on how to screen cascading funding companies is lacking; and in general, recommend a secure by design approach in projects implementation for systemic security. Especially in large European consortium, it is crucial that all partners have the same measures and understanding of risks and adopt best practices.
3. **Develop a voluntary training programme leading to certification, based on these recommendations, at EU level in research security practices for RPOs**: (currently partially included under ethics and data management but not enough yet, considering the current geopolitical and geoeconomical risks), along the lines of the excellence in research certification. The HRS4R | EURAXESS (europa.eu) as a way to implement best practices.
4. **Support the creation of secure national and EU platforms for exchange of best practices:** for governments, and their agencies, private sector, RPOs and academia as appropriate to discuss developments in research security.

EARTO remains ready to provide additional input on each topic mentioned above: our experts are available for further discussion with the EU institutions to ensure that a proper framework is given to research security in Europe.

EARTO - European Association of Research and Technology Organisations

Founded in 1999, EARTO promotes RTOs and represents their interest in Europe. EARTO network counts over 350 RTOs in more than 31 countries. EARTO members represent 150,000 highly-skilled researchers and engineers managing a wide range of innovation infrastructures.

RTOs - Research and Technology Organisations

From the lab to your everyday life. RTOs innovate to improve your health and well-being, your safety and security, your mobility and connectivity. RTOs' technologies cover all scientific fields. Their work ranges from basic research to new products and services' development. RTOs are non-profit organisations whose core mission is to produce, combine and bridge various types of knowledge, skills and infrastructures to deliver a range of research and development activities in collaboration with public and industrial partners of all sizes. These activities aim to result in technological and social innovations and system solutions that contribute to and mutually reinforce their economic, societal and policy impacts.

EARTO Working Group RD&I Programmes*: is composed of more than 160 experts. This WG is looking at the implementation of the EU RD&I Framework Programmes (Horizon 2020 & Horizon Europe), focusing on monitoring their elaboration, simplification and evaluation. This WG is also looking at how RTOs can be involved in and benefit from projects under the European Digital Programme as well as the European Structural and Investment Funds, but also the role of RTOs in Smart Specialisation Strategies as well as the synergies between the Cohesion Policy and the EU RD&I Programmes.*

EARTO Contact*:* www.earto.eu